APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,929	06/06/2000	IAN R FAIRMAN	36-1334	9644

7590	03/16/2005

NIXON & VANDERHYE
1100 NORTH GLEBE ROAD
8TH FLOOR
ARLINGTON, VA 22201-4714

EXAMINER
HA, LEYNNA A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/555,929	FAIRMAN ET AL.
	Examiner	Art Unit
	LEYNNA T. HA	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-16,21-26 and 29-31* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-16,21-26 and 29-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *11/8/2004*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   Claims 1,4-16,21-26 and 29-31 have been re-examined.   The RCE 11/8/2004

requests the consideration of amendment filed After Final 9/29/2004. However, the set

of claims 1-36 in paper 9/29/2004 is intended for application 09/555,839.   Therefore,

Examiner reconsiders claims 1,4-16,21-26 and 29-31 in paper 3/22/2004.

2.   Claims 1,4-16,21-26 and 29-31 are rejected under 35 U.S.C. 102(e).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of

1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of

2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA

35 U.S.C. 102(e)).

3.   **Claims 1,4-16,21-26 and 29-31 are rejected under 35 U.S.C. 102(e) as being**

anticipated by Iverson, Et Al. (US 5,852,664).

As per claim 1:

Iverson, Et Al. teaches a method of distributing digitally encoded data, comprising:

a)   dividing said data into a multiplicity of frames, **(col.3, lines 18-21)**

b)   encrypting said frames, **(col.4, lines 42-43)**

c)   distributing multiple copies of the said data frames to multiplicity of users, each frame being distributed with a control field **(col.3, lines 38-44 and col.4, lines 51-52)**

d)   communicating a seed value for key generation to respective secure modules located at each of the multiplicity of users, **(col.9, lines 63-64)**

e)   decoding the data frames at respective users using keys derived from the seed value communicated to the secure module, the secure module being arranged to enable decryption of a respective frame only when said control field has been passed to the secure module **(col.3, lines 51-61 and col.9, lines 15-33)**

f)   passing a control message, for modifying and controlling the availability of keys, in the control field to the secure module at a selected one or more users, **(col.3, lines 46-50)**

g)   at the secure module of the or each of selected user, in response to the said control message, controlling the availability of keys generated from the said seed value **(col.9, lines 50-54)**, thereby controlling access by the users to the said data. **(col.2, lines 41-43 and col.8, lines 56-58)**

As per claim 4:   See col.3, lines 54-56; discloses each data frame includes a frame identity field, and each key generated by the secure module is specified to one frame identified by the said field.

As per claim 5:   See col.9, lines 35-39; discloses the step of distributing multiple copies of the said data comprises multicasting packets of data via a communications network to the plurality of users.

As per claim 6:   See col.2, lines 61-62; discloses a control message is distributed with a data frame to the multiplicity of users, a user identity field identifying a selected user or group of users is included in the control message, and the control message is acted on only by the user or group of users identified by the said user identity field.

As per claim 7:   See col.8, lines 39-46; discloses a control message includes a stop flag, and in response to the stop flag the generation of keys at the or each selected user is stopped.

As per claim 8:   See col.7, lines 65-67; discusses returning a response signal from the secure module to the source of the control message.

As per claim 9:   See col.7, lines 60-67; discloses a control message includes a contact sender flag, and the step of returning a response signal from the secure module is carried out when the contact sender flag is set.

As per claim 10:   See col.7, lines 52-58; discusses transmitting a further control message to the user on receipt of the said response signal.

As per claim 11:

Iverson teaches a method of operating a customer terminal in a data communications system, the method comprising:

a)   receiving at the customer terminal a multiplicity of encrypted data frames **(col.4, lines 42-43)**, each with a control field **(col.3, lines 38-44 and col.4, lines 51-52)**

b)   receiving at the customer terminal a seed value for key generation **(col.9, lines 63-64)**

c)   passing said seed value for key generation to a secure module located at the customer terminal, **(col.10, lines 2-7)**

d)   generating in the secure module using the seed value keys for decryption of data frames; **(col.3, lines 51-61 and col.9, lines 15-33)**

e)   decrypting using keys only those respective data frames for which a control field has been received; **(col.10, lines 17-25)**

f)   passing to the said secure module a control message received in the control field; and **(col.3, lines 46-50)**

g)   in response to the said control message controlling the availability of keys generated from the said seed value **(col.9, lines 50-54)**, thereby controlling access by the users to the said data. **(col.2, lines 41-43 and col.8, lines 56-58)**

As per claim 12:

Iverson teaches a method data communications system comprising:

a)   a remote data source arranged to output a plurality of frames, **(col.3, lines 18-21)**

b)   encryption means for encrypting the plurality of frames with different respective keys, **(col.4, lines 42-43)**

c)   communications channel arranged to distribute multiple copies of the encrypted data frames, each with a control field; **(col.3, lines 38-44 and col.4, lines 51-52)**

d)   multiplicity of customer terminals arranged to receive from the communications

channel respective copies of the encrypted data frames,   **(col.9, lines 35-39)**

e)   a key generator located at a customer terminal and programmed to generate

from a seed value keys for use in decrypting data frames; **(col.9, lines 63-64)**

f)   a key control means connected to the key generator, the key control means

comprising:

an interface for receiving the control fields; and **(col.5, lines 57-58)**

control means arranged to only release keys for decrypting those respective

frames for which a control field is received and being arranged to, in response to the

said control messages in control fields, control the availability to the user of keys

generated from the seed value; and **(col.7, lines 42-66)**

g)   decryption means connected to the key generator and arranged to decrypt the

data frames received at the customer terminal from the communications channel.

(col.3, lines 51-54 and col.5, lines 32-46)

As per claim 13:   See col., lines ; discusses the communications channel is a packet-

switched data network.

As per claim 14:

Iverson teaches a customer terminal for use in a method according to any one of claims

1 to 11, the customer terminal comprising:

a)   a data interface for connection to a data communications channel; **(col.5, lines
32-46)**

b)   a key generator programmed to generate from a seed value keys for use in decrypting data frames: **(col.9, lines 63-64)**

c)   decryption means connected to the data interface and key generator and arranged to decrypt data frames received via the data interface **(col.7, lines 17-21)**

d)   a key control means connected to the key generator, the key control means comprising:

an interface for receiving control fields; and   **(col.5, lines 57-58)**

control means arranged to only release keys for decrypting those respective frames for which a control field;   the control means being arranged to in response to control messages in control fields, control the availability to the user of keys generated from the seed value. **(col.3, lines 51-54 and col.5, lines 32-46)**

As per claim 15:

Iverson teaches a data server for use in a method comprising:

a)   a data interface for connection to a data communications channel; **(col.5, lines 26-28)**

b)   means for outputting encrypted data frames with control fields via the data interface onto the communications channel for receipt by a multiplicity of customer terminals;   **(col.4, lines 42-43 and col.5, lines 57-58)**

c)   means for outputting the control fields having control messages onto a data communications channel for controlling the operation of key generators at customer terminals. **(col.3, lines 51-54 and col.5, lines 32-46)**

As per claim 16:   See **col.9, lines 63-64;** discusses generating keys from the seed value by iterated operations on a seed value by selected ones of a plurality of predetermined functions.

As per claim 21:   See col.3, lines 34-36; discloses applying different characteristic variations to data decrypted at different respective customer terminals.

As per claim 22:   See col.5, lines 41-42; discusses the plurality of remote data sources, each outputting a respective plurality of frames.

As per claim 23:   See col.5, lines 57-58; discusses the customer terminal receives a primary seed value common to different respective data streams from the plurality of data sources, and derives from the common primary key a plurality of different respective secondary seed values for decrypting frames from different respective data sources.

As per claim 24:   See col.3, lines 35-37 and col.9, lines 55-64; discusses the data received from different data sources includes different respective source identity values, and the respective secondary seed value is generated from the primary seed value by modifying the primary seed value with the source identity value.

As per claim 25:   See col.3, lines 52-54; discloses each data frame includes a frame type field.

As per claim 26:   See col.4, lines 25-38; teaches a method for storing a receipt including data from the frame type field.

As per claim 29:   See col.8, lines 39-46; discussing the control message received by the secure module causes the secure module to cease releasing keys.

As per claim 30:　　See col.8, lines 39-46; discussing the control message received by the secure module causes the secure module to cease releasing keys.

As per claim 31:　　See col.8, lines 39-46; discussing the control message received by the key control causes the key control to cease releasing keys.
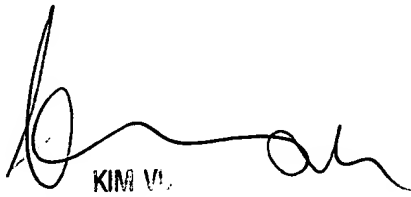
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM V!.
SUPERVISORY P... F...
TECHNOLOGY ......